IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Newport News Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No. 4:16cr16
	)	
EDWARD JOSEPH MATISH III,	)	
	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S THIRD MOTION TO SUPPRESS

Now comes the United States of America, by and through attorneys, Dana J. Boente, United States Attorney for the Eastern District of Virginia, and Kaitlin C. Gratton and Eric M. Hurt, Assistant United States Attorneys, and submits its response in opposition to the defendant, EDWARD JOSEPH MATISH III's Third Motion to Suppress information identifying his home computer recovered pursuant to a search warrant that authorized the use of a network investigative technique to recover such information. For the reasons set forth below, the defendant's motion should be denied.

INTRODUCTION

After a months-long investigation, the Federal Bureau of Investigation (FBI) briefly assumed administrative control of "Playpen," a website dedicated to the sharing of child pornography. The FBI also sought and obtained a warrant from the Honorable Theresa Carroll Buchanan, United States Magistrate Judge for the Eastern District of Virginia permitting it to use a "Network Investigative Technique" (the "NIT") during that same period, which would cause a computer logging into Playpen to reveal certain identifying information—most importantly, its

concealed Internet Protocol (IP) address. Once this warrant, as well as authorization to monitor site users' communications, was obtained, Playpen was hosted from a government-controlled computer server located in the Eastern District of Virginia. Playpen's content was augmented with computer instructions comprising the NIT. Such content, including the NIT, remained on the server in the Eastern District of Virginia until a site user or administrator accessed the site's content at that location and downloaded it. Thus, the deployment of the NIT also occurred within the Eastern District of Virginia.

Among the IP addresses identified accessing Playpen was one associated with defendant Edward Joseph Matish III ("the defendant"). Following the execution of a search warrant at the defendant's home in Newport News, Virginia, located within the Eastern District of Virginia, the defendant was indicted and arrested on charges of access with intent to view child pornography involving a prepubescent minor. The defendant was later charged with additional counts of receipt of child pornography.

The defendant has filed several pretrial motions, including two motions to suppress the identifying information returned by the NIT. In his First Motion to Suppress, the defendant challenged the sufficiency, scope, and—in a very limited sense—execution of the NIT authorized by the same warrant that is the subject of the instant motion. He also requested a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154, 156 (1978), claiming that the warrant's affiant intentionally or recklessly misled the issuing court about how Playpen appeared. In the instant motion, the defendant claims that Judge Buchanan lacked authority to authorize the NIT warrant under the Federal Magistrates Act (28 U.S.C. § 636) and Federal Rule of Criminal Procedure 41(b) and, therefore, that the NIT warrant was issued void *ab initio*. For the reasons that follow, the defendant's motion should be denied.

The United States incorporates and respectfully refers this Court to the Government's Response to Defendant's First Motion to Suppress (ECF No. 24) for a more detailed factual background of the investigation, the Tor network, and the Playpen website.

LAW

The Federal Magistrates Act establishes the jurisdiction and powers of United States magistrate judges. It provides that "[e]ach United States magistrate judge serving under [it] shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law" certain powers and duties, including "all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a)(1). Federal Rule of Criminal Procedure 41(b) authorizes magistrate judges to issue warrants "[a]t the request of a federal law enforcement officer or an attorney for the government" under a variety of circumstances. Fed. R. Crim. P. 41(b).

DISCUSSION

The defendant argues in the instant motion that (1) Judge Buchanan lacked jurisdiction to authorize the NIT warrant because that warrant allegedly exceeded territorial limits placed on the geographic areas in which a magistrate judge has jurisdiction to issue warrants; and (2) that the issuance of the NIT warrant violated Rule 41 of the Federal Rules of Criminal Procedure. He contends that suppression of the information transmitted by the NIT is appropriate based on these alleged violations. The defendant is wrong on both points and suppression is not warranted.

I. The Magistrate Judge Had Jurisdiction to Issue the NIT Warrant as Applied to the Defendant

First, and most importantly, there is no question that Judge Buchanan had authority to authorize the search conducted in this case. Rule 41(b) authorizes "a magistrate judge with authority in the district . . . to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). In this case, that is precisely what occurred. The warrant authorized the NIT to cause "an activating computer – wherever located – to send a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer, as described above and in Attachment B." Gov't Resp. to Def.'s First Mot. to Suppress, Ex. 1 at 29-30, ¶ 46(a) (ECF No. 24). The defendant and his computer, at all times relevant to the charges against him, were also located in the Eastern District of Virginia. Thus, the defendant's "activating computer" was located within the Eastern District of Virginia when he downloaded the computer instructions comprising the NIT from a server also located in the Eastern District of Virginia. In the same district, Judge Buchanan authorized the inclusion of the NIT in the content the defendant downloaded. Rule 41(b)(1) vests her with authority to issue warrants to search for and seize property located within the District, including the information identifying the defendant's computer identified through the NIT. Information obtained from that NIT, specifically an IP address associated with the defendant, led law enforcement to obtain a search warrant for the defendant's home in Newport News, Virginia, was within the Eastern District of Virginia. There is no doubt that the magistrate who issued the warrant authorizing the NIT had clear authority to do so pursuant to Rule 41(b) as applied to the defendant in this case. Accordingly, Judge Buchanan's issuance of

the warrant pursuant to which that information was obtained did not contravene Rule 41(b). Similarly, the Magistrate Judge had authority to authorize to issue the NIT warrant in this case, even the narrowest plain reading of the Federal Magistrates Act.

The defendant can make no plausible argument that the Magistrate Judge who issued the NIT warrant did not have jurisdiction to authorize a search or seizure of information from his computer, nor can he possibly show any prejudice resulting from the execution of that warrant. Instead, he argues that because "[t]he FBI did not know the physical location of any computer . . . until after the search was completed," the fact that the defendant's computer was located in the Eastern District of Virginia "cannot cure the *ex ante* jurisdictional flaw that infected the NIT Warrant at its inception." Def.'s Third Mot. to Supp. at 15 (ECF No. 34). No court in any related case has adopted such a restrictive reading of Rule 41(b)(1) or the Federal Magistrates Act. Courts that have considered the NIT warrant in related cases have repeatedly cited the location of the defendant and his computer when analyzing whether Rule 41(b)(1) provided Judge Buchanan with the authority to issue the warrant. *See United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) (rejecting an argument that the NIT warrant complied with Rule 41(b)(1) "because the object of the search and seizure was Mr. Michaud's computer, not located in the Eastern District of Virginia."); *United States v. Stamper*, No. 1:15-CR-109 (MRB), ECF No. 48 at 21-23 (S.D. Ohio Feb. 19, 2016) (same); *United States v. Levin*, No. 15-10271-WGY, 2016 WL 1589824, at *5 (D. Mass. Apr. 20, 2016) (same); *United States v. Arterbury*, No. 15-CR-182-JHP, ECF No. 42 (N.D. Okla. Apr. 25, 2016) ("Subsection 41(b)(1) does not provide authority for the Virginia warrant because Arterbury's computer was not located in or seized in the Eastern District of Virginia."). If an *ex post* determination that a computer was located outside the Eastern District of Virginia is

appropriately considered when determining whether the NIT warrant was authorized under Rule 41(b)(1), then the same *ex post* determination that a computer was located within the Eastern District of Virginia is also proper and relevant to such a determination. Here, it is sufficient to conclude the Court's inquiry, because the computer was in the same district as the magistrate who authorized the use of the NIT to identify and locate it.

II. The Defendant Lacks Standing to Raise the Argument that the Magistrate Judge Lacked Jurisdiction Outside the Eastern District of Virginia

The defendant cannot vicariously assert the rights of individuals outside the Eastern District of Virginia to create a defect where none otherwise exists. Put simply, he lacks standing to make any argument regarding how the issuance of the NIT warrant would apply to a third party found outside of the Eastern District of Virginia. The government does not concede that the issuance of the NIT warrant exceeded the magistrate's authority—even as applied to a subject found outside of the Eastern District of Virginia—however, the defendant in this case cannot raise that argument. Both the defendant and the magistrate judge who issued the NIT warrant are located in the Eastern District of Virginia.

The Fourth Amendment affords individuals the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. However, the scope of that right is limited. The Supreme Court has long insisted that "Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (collecting cases). When assessing an alleged violation of the Fourth Amendment, "the question is whether the challenged search or seizure violated the Fourth Amendment rights of a criminal defendant who seeks to exclude the evidence obtained during it." *Id.* This inquiry "requires a determination

of whether the disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect." *Id.* "A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed" and therefore is not entitle to benefit from the exclusionary rule's protections. *Id.* at 134 (citing *Alderman v. United States*, 394 U.S. 165, 174 (1969)).

The defendant has no privacy interest in any property found as a result of the NIT warrant that is not his own property, and therefore no standing to raise the argument that Judge Buchanan lacked jurisdiction to issue the warrant as applied to individuals outside the Eastern District of Virginia.

III. The Issuance of the NIT Warrant was Lawful

Even if the defendant could argue that the NIT warrant was defective under the Federal Magistrates Act and Federal Rule of Criminal Procedure 41 because it authorized the use of the NIT to identify and locate computers outside the Eastern District of Virginia, he would not prevail. The 31-page NIT warrant affidavit amply articulated—and Judge Buchanan found—probable cause to deploy the NIT to registered users of a website dedicated to the advertisement and distribution of child pornography that operated on the anonymous Tor network. The warrant particularly described exactly what information would be collected through the NIT—seven discrete items of identifying information—and how that information would assist with identifying Playpen users and administrators. In so doing, it comprehensively established a fair probability that evidence of a crime would be found through the issuance and execution of the warrant. Moreover, the NIT warrant was issued by a magistrate judge within the jurisdiction of the District in which the website operated during the period of authorization

and, accordingly, the District into which registered site users reached when accessing the website.

As a threshold matter, the defendant's arguments concerning the magistrate judge's authority to authorize the NIT warrant should be placed in context and their ramifications laid bare. When the government sought the NIT warrant, thousands of Playpen users were using Playpen to access and share child pornography as well as to facilitate ongoing abuse of children. Playpen was set up to conceal their identities. The defendant does not claim that the government should (or could) have sought a warrant elsewhere. He also does not suggest that the government should have more scrupulously hewn to the procedures contained in Rule 41 for obtaining and executing a warrant. Rather, he maintains that his use of a Tor hidden service dedicated to the sharing of child pornography denies any court in any jurisdiction authority to issue a search warrant under the Federal Magistrates Act and Rule 41 necessary to identify him. The defendant's arguments are without merit.

A. The Issuance of the NIT Warrant Does Not Violate the Federal Magistrates Act

Even if—assuming *arguendo*—the defendant could argue that Judge Buchanan lacked authority to issue a warrant to search or seize information from his computer when that computer was located within the Eastern District of Virginia, the issuance of the NIT warrant comported with the Federal Magistrates Act (28 U.S.C. § 636). The plain language of § 636(a) vests a United States magistrate judge with certain powers and duties, including those "conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a)(1). Under the Federal Magistrates Act, a magistrate judge "shall have" such powers "within the district in which sessions are held by the court that appointed the magistrate

judge, at other places where that court may function, and elsewhere as authorized by law." 28 U.S.C § 636(a). The prepositional phrase beginning "within the district" modifies the verb "shall have," which immediately proceeds that phrase—not the enumerated powers that follow it. Thus, Section 636(a) limits where a magistrate judge may possess such powers, but not necessarily where those powers can have effects. In the warrant context, this means that the warrant must *issue* from a district described in § 636(a)—for example, the district in which a magistrate judge sits—but not that the warrant's effects must be limited to that district.

The defendant's mistaken assumption is that a magistrate judge cannot possess a power that has effects beyond the places described in § 636(a). Indeed, even a cursory review of Rule 41(b) makes clear that the narrow reading of § 636(a) the defendant urges is inapposite. For example, Rule 41(b)(2) expressly provides that "a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district[.]" Fed. R. Crim. P. 41(b)(2). Although Rule 41(b)(2) requires that such person or property must be "located within the district when the warrant is issued," it nevertheless shows that a magistrate judge can exercise power with precisely the same out-of-district effects—namely, a search or seizure—that the defendant asserts contravene the territorial jurisdiction provided her by § 636(a). *Id.* Indeed, nearly every provision of Rule 41(b) underscores the absurdity of the jurisdictional limits the defendant proposes. Save Rule 41(b)(1), all authorize the issuance of warrants for either persons, property, or both with potential or explicit out-of-district effects. For example, Rule 41(b)(3) authorizes a magistrate judge "in any district in which activities related to . . . terrorism may have occurred . . . to issue a warrant for a person or property within or outside that district." Fed. R. Crim. P. 41(b)(3). Rule 41(b)(4) allows a magistrate judge "to issue a warrant to install within the district a tracking device" that can be used "to track the movement of a person or

property located within the district, outside the district, or both." Fed. R. Crim. P. 41(b)(4). And Rule 41(b)(5) authorizes a magistrate judge "in any district where activities related to the crime may have occurred" or—without any showing that activities related to the crime might have occurred in that district—a magistrate judge in the District of Columbia to "issue a warrant for property that is located outside the jurisdiction of any state or district but within" a number of other places, including any "United States territory, possession, or commonwealth." Fed. R. Crim. P. 41(b)(5). Were the Court to adopt the cramped reading of § 636(a) that the defendant proposes, the issuance of a warrant in accordance with all but one of Rule 41(b)'s provisions would violate the Federal Magistrates Act because such a warrant would authorize the "exercise of power over places that me[e]t none of § 636(a)'s self-contained geographic criteria." Def.'s Third Mot. to Supp. at 5. Were that true, a magistrate judge could not exercise powers and duties explicitly conferred by a Rule of Criminal Procedure, as provided for by § 636(a)(1), without violating the same provision of the Federal Magistrates Act that vests her with such powers. The absurdity of this result and the plain language of § 636(a) make clear that the Federal Magistrates Acts limits only the district in which a United States magistrate judge may possess her powers and not the place where those powers can have effect.

None of the authority on which the defendant relies to support his argument that the issuance of the NIT warrant violated the Federal Magistrates Act is persuasive or precedential. First, the concurring opinion in *United States v. Kreuger*, 809 F.3d 1109 (10th Cir. 2015) is not binding on this Court, nor—for that matter—on any court. For all of the reasons set forth above, this concurring opinion espouses an incorrect reading of § 636(a). Further, the facts at issue in *Kreuger* are easily distinguishable from the facts here. There, a magistrate judge in Kansas issued a search warrant for physical property known to be located in Oklahoma. In the

instant case, a magistrate judge issued a warrant allowing the content of a website hosted in her district to be augmented with additional computer instructions comprising the NIT, which would be downloaded from the server in that district by users and administrators accessing the site. Finally, the *Kreuger* concurrence's reasoning does not apply to this case, because the defendant was located in the same district as the magistrate who issued the NIT warrant. For the same reason, neither the *Levin* nor the *Arterbury* opinions are instructive. Neither bind this Court's consideration of the NIT warrant and both concerned the application of that warrant to defendants found outside the Eastern District of Virginia.

Judge Buchanan's issuance of the NIT warrant complied with the Federal Magistrates Act because the she authorized that warrant within the district in which sessions are held by the court that appointed her (as opposed to another district in which she happened to be located) and the issuance of such a warrant fell within the powers and duties conferred on her by the Rules of Criminal Procedure for the United States District Court. Accordingly, Judge Buchanan did not act beyond her authority under the Federal Magistrates Act when she authorized the NIT warrant.

B. The Issuance of the NIT Warrant Does Not Violate Rule 41

As set forth in detail above, the issuance of the NIT warrant did not violate Rule 41 in this case because the defendant—and his computer—were located within the Eastern District of Virginia at all times relevant to the investigation, the same district as the magistrate judge who authorized the warrant. Accordingly, the execution of that warrant and resulting identification of information identifying the defendant's computer did not contravene Rule 41(b)(1) nor even the narrowest reading of the Federal Magistrates Act. The defendant cannot vicariously assert

the rights of other Playpen users located outside this District to create a violation or constitutional defect where none otherwise exists.[1]

Even if—assuming *arguendo*—the defendant could argue that the magistrate judge lacked authority to issue a warrant to search or seize information from his computer when that computer was located within the Eastern District of Virginia, the issuance of the NIT warrant otherwise comported with the provisions of Rule 41(b).

Rule 41(b) is flexible enough to allow the issuance of warrants to investigate Tor hidden services.[2] *See United States v. New York Telephone Co.*, 434 U.S. 159, 169 & n.16 (1977). In fact, three separate provisions support the issuance of the NIT warrant.

First, Rule 41(b)(4) allows a magistrate judge "to issue a warrant to install within the district a tracking device." Fed. R. Crim. P. 41(b)(4). Such a "warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." *Id.* A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Fed. R. Crim. P. 41(a)(2)(E); 18 U.S.C. § 3117(b). In a physical tracking device case, investigators might obtain a warrant to install a tracking device in a container holding contraband, and investigators might

[1] Again, the government does not concede that any such violations or defects exist in cases involving users located outside the Eastern District of Virginia.

[2] In order to eliminate any ambiguity on this issue, the Advisory Committee on Criminal Rules has endorsed an amendment to Rule 41 to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media and to seize or copy electronically stored information" inside or outside of an issuing district if, among other things, "the district where the media or information is located has been concealed through technological means." *See* Advisory Committee on Rules of Criminal Procedure, May 2015 Agenda, at 107-08 (available at http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015). The amendment has been approved by the Advisory Committee on Criminal Rules, the Standing Committee, and the Judicial Conference of the United States. *See* Transmittal of Proposed Amendments to the Federal Rules at 8 (available at http://www.uscourts.gov/rules-policies/pending-rules-amendments). On April 28, 2016, the Supreme Court adopted the amendment and transmitted it to Congress. *Id.* Absent congressional action, the amendment will take effect on December 1, 2016. *See* April 28, 2016 Rules of Criminal Procedure Term Order at 3 (available at http://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf). The defendant cites this amendment in support of his contention that deliberate violation of Rule 41(b) occurred in this case. That argument will be addressed below.

then determine the location of the container after the targets of the investigation carry the container outside the district. *See United States v. Knotts*, 460 U.S. 276, 285 (1983) (upholding against a Fourth Amendment challenge the use of a "beeper" that had been placed in a container of chloroform, allowing law enforcement to monitor the location of the container); *United States v. Karo*, 468 U.S. 705, 712 (1984) (upholding the installation of a beeper in a container belonging to a third party, holding that the defendant accepted the container as it came to him and was not entitled to object to the beeper's presence even though it was used to monitor the container's location); *United States v. Jones*, 132 S. Ct. 945, 952-53 (2012) (requiring a search warrant for the installation of an information-gathering device to property belonging to a defendant). In this case, the NIT functioned in a similar manner in the context of the Internet. After obtaining a warrant from a neutral and detached magistrate judge sitting in the Eastern District of Virginia, investigators augmented the illicit content of the Playpen site—hosted on a computer server located in that same district—with additional computer instructions comprising the NIT. When the defendant logged in to Playpen by entering his username and password and retrieved information from that server, he affirmatively retrieved both the illicit content and the NIT. Once downloaded, the NIT sent law enforcement information concerning the computer on which it and the illicit content were located. Investigators used this information to identify and locate the defendant. Thus, Rule 41(b)(4) provided sufficient authority to issue the NIT warrant regardless of the location of the user or his computer. The application of Rule 41(b)(4) is particularly appropriate when the NIT was retrieved by a user located within the District in which the warrant authorizing it was obtained, because under any reading of the Rule and its application, the NIT was installed within the issuing district.

Second, Rule 41(b)(2) allows a magistrate judge "to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Fed. R. Crim. P. 41(b)(2). Here, the warrant authorized use of the NIT (a set of computer instructions) located on a server in the Eastern District of Virginia when the warrant was issued. Gov't Resp. to Def.'s First Mot. to Supp., Ex. 1 at 22-23, 24 ¶¶ 30, 33. As Rule 41(a)(2)(A) defines "property" to include both "tangible objects" and "information," the NIT constituted property within the District from which the warrant issued. Moreover, the NIT was only retrieved by registered users of Playpen who logged into the website, located within the Eastern District of Virginia, with a username and password. *Id.*, Att. A. Each of those users—including the defendant—accordingly reached into this District's jurisdiction to access the site (and the child pornography therein augmented with the NIT). Thus, Rule 41(b)(2) also provided sufficient authority to issue the warrant for use of the NIT regardless of the location of Playpen users and their computers. Again, the applicability of this Rule is underscored in this case, where the defendant and his computer were, at all times relevant to the investigation, within the District from which the NIT warrant issued. Thus, even under a narrow reading of the authority provided by Rule 41(b)(2) limited to the search or seizure of the defendant's computer and identifying information therefrom, all such information was within the district at the time the NIT warrant issued. The possibility that such property or information "might move or be moved outside the district before the warrant [wa]s executed" is expressly provided for by the Rule. Accordingly, Rule 41(b)(2) provides a second, independent basis supporting the issuance of the NIT warrant.

Finally, the NIT warrant was issued by a magistrate judge in the district with the strongest known connection to the search: all Playpen users entered this District by accessing the Playpen server here, retrieved content from that server that included illicit images of child pornography (augmented with computer instructions comprising the NIT), and the NIT sent limited information back to a server in that district. The magistrate judge had authority under Rule 41(b)(1) to authorize a search warrant for "property located within the district." The use of the Tor hidden service by the defendant and other Playpen users made it impossible for investigators to know in what other districts, if any, the execution of the warrant would take place. In these circumstances, it was reasonable for the Eastern District of Virginia magistrate judge to issue the warrant. Interpreting Rule 41 to allow the issuance of warrants like the NIT does not risk significant abuse, because, as with all warrants, the manner of execution "is subject to later judicial review as to its reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979). Indeed, for the reasons outlined above, the NIT warrant certainly complied with Rule 41(b)(1) as applied to this defendant. Accordingly, this Court should conclude that the issuance of the warrant did not violate Rule 41.

To support his argument to the contrary, the defendant cites a magistrate judge's opinion holding that Rule 41(b) does not authorize the issuance of a warrant for use of a different—and significantly more invasive—NIT than the one used in this case. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). *In re Warrant*, though, does not undermine Judge Buchanan's decision to issue the warrant here. As a threshold matter, the case is an outlier. To the government's knowledge, in every other matter involving an application for a search warrant to identify a person hiding his identity and location using Internet anonymizing techniques, the judge has issued the warrant. *See, e.g., United*

States v. Cottom, et al., No. 13-cr-108 (D. Neb. Oct. 14, 2014) (ECF No. 122, Attach. 1; ECF No. 123, Attach. 1) (authorizing two separate NIT search warrants), (ECF No. 155) (denying suppression motion); *United States v. Welch*, 811 F.3d 275 (8th Cir. 2016) (affirming denial of suppression motion in a related case); *In re Search of NIT for Email Address texas.slayer@yahoo.com*, No. 12-sw-5685 (D. Col. Oct. 9, 2012) (ECF No. 1) (search warrants); *In re Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government*, No. 17-mj-5114 (W.D. Wash. June 12, 2017), *available at* http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf.

Moreover, the reasoning of the Texas magistrate judge's decision in *In re Warrant* does not apply to the use of the NIT in this case. That court correctly found it "plausible" that the NIT fell within the definition of a tracking device. 958 F. Supp. 2d at 758. Nevertheless, the court held that Rule 41(b)(4) did not apply because there was not showing that the installation of the NIT software would be within its district. *See id.* That was not the case here: installation of the NIT within the meaning of Rule 41(b)(4) took place on the server in the Eastern District of Virginia. As the analogy to the physical tracking device demonstrates, the government "install[ed]" the NIT within the meaning of Rule 41(b)(4) when it augmented Playpen's content, located on a computer server in the issuing court's district, with the computer instructions comprising the NIT. The defendant's subsequent retrieval of the NIT and its collection of limited information from his computer constituted "use of the device" for purposes of Rule 41(b)(4), regardless of whether that process of collection included any subsequent "installation" on the defendant's computer. Again, even if that were used as the metric, in this case, the installation undisputedly occurred in the issuing court's district.

Even if the defendant could show that Rule 41 did not expressly authorize the search and seizure contemplated by the NIT warrant and accompanying affidavit, the Court is not limited to such a narrow reading of that Rule. Indeed, courts have long read Rule 41 broadly, interpreting it to permit searches where they are consistent with the Fourth Amendment, even in cases involving searches are not explicitly authorized by the text of the Rule. In *United States v. New York Telephone Co.*, for example, the Supreme Court upheld a 20-day search warrant for a pen register to collect dialed telephone number information, despite the fact that Rule 41's definition of "property" at the time did not include information and the fact that Rule 41 required that a search be conducted within 10 days. 434 U.S. 159, 169 & n.16 (1977). The Court explained that Rule 41 "is sufficiently *flexible* to include within its scope electronic intrusions authorized upon a finding of probable cause," and noted that this flexible reading was bolstered by Rule 57(b), which provides, "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." *Id.* at 169-70 (emphasis added).[3] Several Circuits have similarly construed Rule 41 broadly to allow warrants not explicitly authorized by the plain language of the Rule. For example, in *United States v. Koyomejian*, the Ninth Circuit interpreted Rule 41 broadly to allow prospective warrants for video surveillance, despite the absence of provisions in Rule 41 explicitly authorizing or governing such warrants. 970 F.2d 536, 542 (9th Cir. 1992). The Seventh Circuit observed in *United States v. Torres* that denying courts the authority to issue warrants for searches consistent with the Fourth Amendment would encourage warrantless searches justified by claims of exigency:

[3] Rule 57(b) now provides: "A judge may regulate practice in any manner consistent with federal law, these rules, and the local rules of the district."

> [H]olding that federal courts have no power to issue warrants authorizing [an investigative technique] might . . . simply validate the conducting of such surveillance without warrants. This would be a Pyrrhic victory for those who view the search warrant as a protection of the values in the Fourth Amendment.

751 F.2d 875, 880 (7th Cir. 1984). The strong preference for reading Rule 41 broadly goes a long way to undercut the defendant's claim that the magistrate's authorization of the NIT warrant violated that Rule, even were the Court to find that the rule did not expressly authorize the use of the NIT as described.

IV. The NIT Warrant was Reasonable Under the Fourth Amendment

The NIT warrant falls with the broad and flexible provisions of Rule 41, both as a general matter and with respect to the defendant, specifically. A detached and neutral magistrate judge, appropriately exercising her authority under the Federal Magistrates Act, found probable cause to support the use of the NIT to identify Playpen users and administrators. The warrant particularly described the places to be searched and the limited information to be seized. In doing so, it comprehensively established a fair probability that evidence of a crime would be found through its execution. The defendant makes much of his strained readings of both § 636(a) and Rule 41, arguing that they support the conclusion that Judge Buchanan acted beyond her authority and, therefore, her jurisdiction when she authorized the NIT warrant, rendering that warrant void and, therefore, "no warrant at all." Def.'s Third Mot. to Supp. at 1-2 (ECF No. 34). Even if the defendant were correct, that would not end the inquiry because a warrantless search does not amount to a per se Fourth Amendment violation, without exception. Instead, the question is whether the use of the NIT was nevertheless reasonable under the Fourth Amendment. In this context, it undoubtedly was.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. The ultimate touchstone of the Fourth Amendment is reasonableness. *Riley v. California*, 134 S. Ct. 2473, 2482 (2014). When law enforcement officials undertake a search to discover evidence of criminal wrongdoing, reasonableness generally requires them to obtain a judicial warrant. *Id.* The Supreme Court has recognized that the presumption that a warrantless search is unreasonable "may be overcome in some circumstances because '[t]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). "One well-recognized exception applies when the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." *Id.* (internal quotation marks omitted). The Fourth Circuit has held that the exigency exception applies when officers "have probable cause to believe that evidence of illegal activity is present and [ ] reasonably believe that evidence may be destroyed or removed before they could obtain a warrant," *United States v. Cephas*, 254 F.3d 488, 494-95 (4th Cir. 2001), or when "speed is essential to prevent escape or harm to police or others." *Mora v. The City of Gaithersburg, MD*, 519 F.3d 216, 226 (4th Cir. 2008). Court's must evaluate "the totality of the circumstances" to determine whether exigencies justified a warrantless search. *Missouri v. McNeely*, 133 S. Ct. 1552, 1559 (2013).

Here, even if the government could not obtain a warrant for use of the NIT that complied with the letter of Rule 41(b), ample exigent circumstances existed to justify its use. Playpen enabled ongoing sexual abuse and exploitation of children, and deploying the NIT against Playpen users was necessary to stop the abuse and exploitation and to identify and apprehend abusers. Such abuse and exploitation included both the online sexual exploitation of children

through the distribution and receipt of child pornography and the ongoing abuse of live victims by "hands on" offenders. For example, undercover reviews of postings related to the use of Playpen's private messages or PMs revealed discussions of such abuse. Gov't Resp. to Def.'s First Mot. to Supp., Ex. 1 at 19, ¶ 21 (ECF No. 24) (describing a post by a user stating, "Yes i can help if you are a teen boy and want to f[***] your little sister, write me a private message."). As of early January 2016, use of the NIT in this investigation had led to the identification or recovery from abuse of twenty-six child victims. Resp. to Order Compelling Discovery at 7-8, *United States v. Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. Jan. 8, 2016) (ECF No. 109) (attached as Government's Exhibit 1). The FBI has also identified at least thirty-five individuals who have been determined to be "hands on" child sexual offenders, and seventeen individuals who have been determined to be producers of child pornography. *Id.*

The information the collected was also fleeting. If law enforcement had not collected IP address information at the time of user communications with Playpen, then, due to the site's use of Tor, law enforcement would have been unable to collect identifying information. Absent the FBI's brief assumption of administrative control and use of the NIT to obtain that information, "the identities of the administrators and users of [Playpen] would [have] remain[ed] unknown" due to the location and operation of Playpen on the anonymizing Tor network. Gov't Resp. to Def.'s First Mot. to Supp., Ex. 1 at 22, ¶ 29 (ECF No. 24). Accordingly, if the warrant could not have been issued, then no warrant could have been obtained in a reasonable amount of time to identify perpetrators. *See United States v. Struckman*, 603 F.3d 731, 738 (9th Cir. 2010) (stating that to invoke the exigent circumstances exception, "the government must . . . show that a warrant could not have been obtained in time").

Moreover, the NIT warrant was minimally invasive and specifically targeted at the fleeting identifying information: it only authorized collection of IP address information and other basic identifiers for site users. As thoroughly explained in the Government's Response to the Defendant's First Motion to Suppress, the defendant does not have a reasonable expectation of privacy in his IP address. ECF No. 24 at 33-35. Before proceeding with a more invasive entry and search of the defendant's home and electronic devices, the government obtained a second Rule 41 warrant.

In sum, the NIT warrant provided authority for use of the NIT, and it is certainly preferable that the government obtain warrants (as it did here) to investigate large criminal enterprises like Playpen. Criminals' use of anonymizing technologies like Tor to perpetuate crimes should not place them beyond the reach of law enforcement (or courts). But even if no court had authority to issue a warrant to use a NIT to investigate Playpen users outside the Eastern District of Virginia, as the defendant essentially argues, its use was nonetheless reasonable under the Fourth Amendment.

V. Suppression is Not an Appropriate Remedy

Suppression is a "last resort, not our first impulse," and any benefit to suppressing evidence (general deterrence of law enforcement misconduct) must outweigh the substantial social cost that results when "guilty and possibly dangerous defendants go free." *Herring v. United States*, 555 U.S. 135, 140-41 (2009); *see also United States v. Stephens*, 764 F.3d 327, 335 (4th Cir. 2014). The real deterrent value "is a 'necessary condition for exclusion,' but it is not a 'sufficient' one." *Davis v. United States*, 131 S. Ct. 2419, 2427 (2011) (quoting *Hudson v. Michigan*, 547 U.S. 586, 596 (2006)). "Exclusion is 'not a personal constitutional right,' nor is it designed to 'redress the injury' occasioned by an unconstitutional search." *Davis*, 131 S.

Ct. at 2426 (quoting *Stone v. Powell*, 428 U.S. 465, 486 (1976)). It is not a "strict liability game." *Id.* at 2429. Accordingly, defendants who seek suppression much clear a "high obstacle," *id.* at 141, and "when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should largely be determined by the preference to be accorded to warrants." *Illinois v. Gates*, 462 U.S. 213, 237 n.10 (1983) (quoting *United States v. Ventresca*, 380 U.S. 102, 109 (1965)). "This reflects both a desire to encourage use of the warrant process by police officers and a recognition that once a warrant has been obtained, intrusion upon interests protected by the Fourth Amendment is less severe than otherwise may be the case." *Id.*

The defendant urges the Court to suppress the identifying information obtained by the NIT, arguing that his narrow (and incorrect) reading of what he terms the territorial limitations of the Federal Magistrate Act and Rule 41(b) support a finding that the warrant's issuance violated the Fourth Amendment or, in the alternative, amounted to a substantive, prejudicial, and deliberate violation of Rule 41(b) warranting suppression. The defendant is wrong on both points.

For the reasons explained above, Judge Buchanan did not exceed the territorial limitations of the Federal Magistrates Act when she authorized the NIT warrant. She signed the warrant "within the district in which sessions are held by the court that appointed [her]." 28 U.S.C. § 636(a). The Federal Magistrates Act required no more. To support his argument that the NIT warrant contravened the bounds of the Fourth Amendment's protections, the defendant argues that "a finding that the magistrate judge acted beyond her authority under Rule 41(b) means that she acted beyond her jurisdiction under § 636(a)." Def.'s Third Mot. to Supp. at 3

(ECF No. 34). In so arguing, the defendant seeks to render *all* violations of Rule 41(b) violations of constitutional import. That is not the standard applicable to such violations.

Assuming *arguendo* that the NIT warrant was somehow deficient under Rule 41, suppression is neither required by law nor reasonable under the circumstances. Although the purpose of Rule 41 is to carry out the mandate of the Fourth Amendment, not all Rule 41 violations render a search invalid. *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000); *United States v. Wyder*, 674 F.2d 224, 226 (4th Cir. 1982). Rule 41 violations fall into two categories: "those involving constitutional violations and all others." *Simons*, 206 F.3d at 403. A constitutional violation occurs only if the violation "renders the search unconstitutional under the fourth amendment." *United States v. Jones*, 822 F.2d 56 (4th Cir. 1987) (unpublished table decision) (citing *United States v. Ritter*, 752 F.2d 435, 441 (9th Cir. 1985)). "Non-constitutional violations of Rule 41 warrant suppression only when a defendant is prejudiced by the violation, or when there is evidence of intentional and deliberate disregard of a provision of the Rule." *Simons*, 206 F.3d at 402 (internal citations and quotation marks omitted).

A. The Issuance and Execution of the NIT Warrant did not Violate the Fourth Amendment

None of the bases that the defendant argues warrant suppression withstand scrutiny. First, there was no violation of constitutional magnitude. The defendant wrongly claims that jurisdictional flaws and other fundamental violations of non-ministerial requirements necessarily involved matters of constitutional magnitude. He is wrong. For all the reasons set forth above, Judge Buchanan's authorization of the NIT warrant did not exceed the authority vested in her by the Federal Magistrates Act. Nor did it contravene either the text or the spirit of Rule 41.

As important, the search and seizure here complied with the Fourth Amendment. The Fourth Amendment demands three things of a search warrant: a warrant must be issued by a neutral magistrate; it must be based on a showing of "probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense"; and it must satisfy the particularity requirement." *Dalia*, 441 U.S. at 255; *see also Jones*, 822 F.2d 55, at *2 (rejecting district court's conclusion that a Rule 41 violation was constitutional when "[a]ll of the fourth amendment's required protections were afforded . . . in th[e] case"). As detailed above and in the Government's Response to the Defendant's First Motion to Suppress, the NIT warrant easily meets these requirements.

The government's actions here were also reasonable under the circumstances. Law enforcement has a substantial interest in identifying users of a massive website trafficking in child pornography and furthering the sexual abuse of children. The court-authorized use of the NIT was necessitated by the Tor-based technology that the defendant and other offenders under investigation used to exploit children, which made it impossible for investigators to know where he was located without first using the NIT. Gov't Resp. to Def.'s First Mot. to Supp., Ex. 1 at 23-24, ¶ 31 (ECF No. 24). The individual privacy interests here were extremely limited, due to the minimally invasive nature of the NIT search and its focus on IP address information over which the defendant lacks a reasonable expectation of privacy. Courts must balance the need for the search against any invasion of individual rights. *Riley*, 134 S. Ct. at 2484. The very fact the government sought and obtained a warrant from a neutral magistrate protected the defendant from an unreasonable search and seizure in violation of his constitutional rights. Obtaining that warrant from a magistrate judge in the district where the website was hosted and

where users, like the defendant, actively retrieved the site's content was eminently reasonable, particularly given the lack of available options.

As previously argued in the Government' Response to the Defendant's First Motion to Suppress (ECF No. 24), even if the NIT warrant does not satisfy the Fourth Amendment, the good faith exception bars suppression here. The NIT warrant affidavit contained no knowingly or recklessly false information that was material to the issue of probable cause. The issuing magistrate judge did not abandon her judicial role. The warrant clearly and particularly described the locations to be searched and the items to be seized. The affidavit made a strong, comprehensive showing of probable cause to use the NIT. Therefore, the agents' reliance on the magistrate judge's authority to issue the warrant was objectively reasonable.

B. Suppression is Not an Appropriate Remedy for Any Alleged Violation of Rule 41(b)

In the absence of a constitutional violation, suppression is appropriate "only when a defendant is prejudiced by the violation, or when there is evidence of intentional and deliberate disregard of a provision of the Rule." *Simons*, 206 F.3d at 402 (internal citations and quotation marks omitted). The defendant's claims of prejudice are nothing more than a re-articulation of his arguments concerning the scope of the magistrate judge's jurisdiction. The defendant, in particular, cannot demonstrate prejudice because he is located in the same district as the magistrate judge who authorized the use of the NIT.

At its core, the defendant's argument is that no court anywhere could have issued the NIT warrant because his use of the Tor network to hide his location prevented law enforcement from determining whether he was in the Eastern District of Virginia prior to executing the NIT warrant. Any deviation from the letter of Rule 41 in this case is the product Playpen's users

(including the defendant) use of Tor to evade law enforcement, not some bad faith on the part of law enforcement in trying to comply with Rule 41.[4] Having already used Tor to shield his location from investigators, under no reasonable analysis should he be permitted to wield it as a sword to defeat the government's ability to obtain judicial authorization to search for the true location from which he accessed child pornography, particularly when he did so from the same district as the magistrate judge who provided that authorization. The Court should not "fault the good faith ingenuity of the officers" in responding to the defendant's use of advanced technology with its own, where "interests protected by the fourth amendment and Rule 41 were safeguarded by the officers . . . even though the methods used were novel." *United States v. Vassar*, 648 F.2d 507, 510 n.2 (9th Cir. 1980).

Likewise, the defendant cannot show that any variance from the text of Rule 41(b) warrants suppression as an intentional and deliberate disregard of the Rule. Suppression is only warranted in the case of a deliberate violation of Rule 41 if that violation occurs in "bad faith." *United States v. Lipford*, 203 F.3d 259, 270 (4th Cir. 2000). The warrant request here was the product of a lengthy investigation by agents who, rather than attempting to avoid compliance with Rule 41, deliberately sought to satisfy the letter of Rule 41 by seeking a warrant in the district with the greatest known connection to the criminal activity. There is no evidence that the agents hid critical information from the magistrate or otherwise prevented the magistrate from having all the necessary information. And there is no evidence or even suggestion that the magistrate judge abandoned her neutral and detached judicial function when evaluating—and authorizing—the warrant request. Rather, law enforcement reasonably concluded that, under

[4] As Judge Bryan found, "[t]he rule does not directly address the kind of situation that the NIT warrant was authorized to investigate, namely, where criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI at a known location." *Michaud*, No. 3:15-cr-0535-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016).

Rule 41, a magistrate judge in the Eastern District of Virginia could issue a warrant to augment a website's content with the NIT when that content was located on a server in the district and would travel outside the district only after individuals—who had undertaken conscious efforts to conceal their location—accessed that server and requested the site's content. And Judge Buchanan agreed. Even if that conclusion were erroneous, such misapprehension can hardly be taken as evidence of "bad faith."[5] *See Jones*, 822 F.2d 56, at *2 (finding "no evidence that any officer intentionally disregarded the mandates of Rule 41" when "all evidence pointed to careful compliance with the rule."). Accordingly, suppressing the highly probative evidence that agents used to identify the defendant is unjustified.

The defendant nonetheless insists that the government committed an intentional violation of Rule 41, pointing to the government's proposal and support of an amendment to the Rule. The proposed amendment to Rule 41 was intended to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." This proposed amendment and the letters in support of it cited by the defendant prove only that the government recognized the need for clarification. They do not reflect a concession that, but for that clarification, Rule 41 is a bar to the approach taken by the government in this case. That the Department of Justice seeks greater clarity in a rule does not convert conduct taken in good faith to a deliberate and intentional violation of that rule.

[5] Indeed, the defendant himself argues that the magistrate judge—not the agents—erred by issuing the warrant. Citing *In re Warrant*, he argues that the magistrate judge should have concluded that she lacked authority to issue the warrant and rejected the application. Def.'s Third Mot. to Supp. at 14. Suppression is not warranted under the exclusionary rule to correct judicial mistakes. *Cf. United States v. Stephens*, 764 F.3d 327, 334 (4th Cir. 2014) ("*Police practices* trigger the harsh sanction of exclusion only when they are deliberate enough to yield meaningful deterrence, and culpable enough to be worth the price paid by the justice system." (quoting *Davis*, 131 S. Ct. at 2427) (emphasis added)).

Moreover, at the time the Department of Justice proposed the Rule 41 amendment, a single magistrate judge—in one case—had rejected a warrant to locate a computer concealed through technological means, but every other magistrate judge known to consider the issue had authorized such a warrant. Accordingly, no evidence exists to support the defendant's contention that agents who scrupulously sought to adhere to the requirements of Rule 41 nevertheless intentionally and deliberately violated it.

CONCLUSION

For the foregoing reasons, the defendant's Third Motion to Suppress the information identifying his home computer recovered pursuant to a search warrant that authorized the use of the network investigative technique should be denied.

Respectfully submitted,

DANA J. BOENTE
UNITED STATES ATTORNEY

By: _____/s/_____
Kaitlin C. Gratton
Eric M. Hurt
Assistant United States Attorneys
Virginia State Bar Nos. 83935, 35765
Fountain Plaza Three, Suite 300
721 Lakefront Commons
Newport News, VA 23606
Phone: (757) 591-4000
Fax: (757)591-0866
Email: kaitlin.gratton@usdoj.gov
EHurt@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 13th day of May, 2016, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Andrew W. Grindrod
Assistant Federal Public Defender
Office of the Federal Public Defender
150 Bousch Street, Suite 403
Norfolk, Virginia 23510
Andrew_Grindrod@fd.org

Richard J. Colgan
Assistant Federal Public Defender
Office of the Federal Public Defender
150 Bousch Street, Suite 403
Norfolk, Virginia 23510
Richard_Colgan@fd.org

_____/s/_____
Kaitlin C. Gratton
Virginia State Bar No. 83935
Assistant United States Attorney
Attorneys for the United States
United States Attorney's Office
Fountain Plaza Three, Suite 300
721 Lakefront Commons
Newport, VA 23606
Phone: 757-591-4000
Email: kaitlin.gratton@usdoj.gov